CalPERS

FTP Encryption / Decryption

<DeliveryDate>

Title	FTP Encryption / Decryption
Project	
Author	
Initiated On	
Filename	
Keywords	
Comments	
Last Saved By	
Last Saved On	

Revision History

Date	Version	Description	Author
02/26/07	0.1	Initial version	Mike Sisler

1. INTRODUCTION

The Encryption Decryption Service is designed to allow an external entity to interact with CalPERS using encrypted data file s. The service allows both inbound and outbound transfer of files using standard PGP encryption. This document outlines the requirements for an external partner to utilize this service.

1.1 External Partner Requirements

Each external user will be provided with two folders on an external FTP CalPERS server. The first folder will be a prod-in folder for transfer of files TO CalPERS (inbound). The second folder will be a prod-out folder for transfer of files FROM CalPERS (outbound).

Inbound files to CalPERS:

- Data files must be encrypted using any PGP software that is compatible with McAfee E-Business Server Version 7.1.1.
- Data files must be uploaded to the **prod-in** folder on CalPERS external ftp server using Binary mode.
- Data file names must be all lower case and must match the data file naming convention discussed later in this document.
- Two files are required for each transaction, one data file and one semaphore file. Data files must have a .pgp file extension. Sempahore files must have a .sem file extension. The semaphore file will have the same name as the data file but with a .sem file extension. The semaphore file is an empty file that indicates that the data file is complete and ready for further processing. Example of a file pair of files sent for each transaction.
  "*filename*.pgp and "*filename*".sem
- The CalPERS Encryption/Decryption service will poll the prod-in folder for files at a pre-determined interval. The .pgp file and the matching .sem file will be deleted when successfully processed. Erroneous files that do not match the above naming requirements will not be processed.

Outbound files from CalPERS:

- Data files will be encrypted using McAfee E-Business Server Version 7.1.1. PGP software.
- Data files will be uploaded to the **prod-out** folder on CalPERS external ftp server using Binary mode.
- Data file names will be all lower case and will match the data file naming convention discussed later in this document.
- Two files will be uploaded for each transaction, one data file and one semaphore file. Data files will have a .pgp file extension. Sempahore files will have a .sem file extension. The semaphore file will have the same name

as the data file but with a .sem file extension. The semaphore file is an empty file that indicates that the data file is complete and ready for further processing. Example of a file pair of files sent for each transaction. "*filename*.pgp and "*filename*".sem

- The CalPERS Encryption/Decryption service will upload encrypted data files to the FTP location at a pre-determined interval.
- The external trading partner will retrieve files from the FTP location at their own pre-determined interval.
- The external partner application will look for a filename with a .sem file extension. This will indicate that a data file with the same name and a .pgp extension is available for processing. At this point, the application can download the data file to the trading partner's system.
- After successfully downloading the data file, the trading partner's process will rename the data file from a .pgp extension to a .fin extension. This renaming process will indicate that the files have been processed and can be deleted. The Encryption/Decryption service will delete the "*filename*".fin file and the "*filename*".sem file during a scheduled cleanup process.

1.2 File Naming Convention

Both inbound and outbound files must adhere to the file naming convention described below.

The standard format for file names:

A) ***yyyymmddhhmiss_sss_p(n).xxx***

Where:

yyyy is the year

mm is the month

dd is the day.

hh is the hours using a 24 hour clock

mi is the minutes

ss is the seconds

sss is the milliseconds, (use 000 if milliseconds can not be produced)

p(n) application specific area of the file name (project defined)

xxx is the file extension (pgp) for all encrypted files